Bull. Malays. Math. Sci. Soc. (2017) 40:1817–1828
DOI 10.1007/s40840-017-0471-2

BULLETIN of the
MALAYSIAN MATHEMATICAL
SCIENCES SOCIETY
http://www.springer.com/mathematics/journal/40840

Moufang Loops of Odd order p^4q^3

Andrew Rajah[1] · **Lois Adewoye Ademola**[1]

Received: 5 May 2015 / Revised: 14 July 2016 / Published online: 2 February 2017

Abstract It is known that all Moufang loops of order p^4 are associative if p is a prime greater than 3. Also, nonassociative Moufang loops of order p^5 (for all primes p) and pq^3 (for distinct odd primes p and q, with the necessary and sufficient condition $q \equiv 1(\text{mod } p)$) have been proved to exist. Consider a Moufang loop L of order $p^\alpha q^\beta$ where p and q are odd primes with $p < q, q \not\equiv 1(\text{mod } p)$ and $\alpha, \beta \in \mathbb{Z}^+$. It has been proved that L is associative if $\alpha \leq 3$ and $\beta \leq 3$. In this paper, we extend this result to the case $p > 3, \alpha \leq 4$ and $\beta \leq 3$.

Keywords Moufang loop · Maximal subloop · Order · Nonassociative

Mathematics Subject Classification 20N05

1 Introduction

A loop $\langle L, \cdot \rangle$ is called a Moufang loop if it satisfies the identity $(x \cdot y) \cdot (z \cdot x) = (x \cdot (y \cdot z)) \cdot x$.

$\langle L, \cdot \rangle$ being a loop has elements of the form $u = (x \cdot y) \cdot z$ and $v = x \cdot (y \cdot z)$ for all $x, y, z \in L$. $\langle L, \cdot \rangle$ is not necessarily associative. So, if x, y and z are fixed elements of L, u and v may be identical or two different elements in L. Whatever

Communicated by Miin Huey Ang.

✉ Lois Adewoye Ademola
loisola@yahoo.com

Andrew Rajah
andy@usm.my

[1] School of Mathematical Sciences, Universiti Sains Malaysia (USM), 11800 Penang, Malaysia

the case, there would exist a unique element $k \in L$ such that $u = v \cdot k$. (If u and v happen to be the same element, then obviously $k = 1$, the identity element). We use the notation $k = (x, y, z)$ since k is nevertheless a function of these three elements, i.e., $(x \cdot y) \cdot z = (x \cdot (y \cdot z)) \cdot (x, y, z)$.

Now since loops by definition have an identity element and [3] has shown that Moufang loops have the inverse property, if $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in L$, the Moufang loop $\langle L, \cdot \rangle$ would be a group.

It has also been observed that fixing the order of a Moufang loop can force it to be an associative Moufang loop.

The aforementioned led to the study of the question:

"Given a positive integer n, can we find a nonassociative Moufang loop of order n?" This is done by using the prime decomposition theorem to write n as a product of positive powers of distinct primes. These primes are usually arrayed from the smallest to the largest.

The progressive and extensive works of Chein, Leong and Rajah solved completely even order Moufang loops. The odd case is still being resolved. The well-known results found so far are those of [3–7], [10–17] and [22–25].

For distinct odd primes p and q, the existence of nonassociative Moufang loops of order pq^3 have been guaranteed in [22] if and only if $q \equiv 1 (\text{mod } p)$. In addition, the existence of nonassociative Moufang loops of order 3^4 [3] and p^5 for primes $p > 3$ [26] have been long established. In fact, these were classified in [18] and [19], whereas the nonassociative Moufang loops of order pq^3 were classified in [4].

Our work is an extension of the result in [25] where it was proved that for odd primes p and q with $p < q$, all Moufang loops of order p^3q^3 are associative if and only if $q \not\equiv 1 (\text{mod} p)$. Since all Moufang loops of order p^4 are associative if and only if p is a prime with $p > 3$ [10], we move on to the next step, i.e., we obtain the following result:

If p and q are primes with $3 < p < q$, then all Moufang loops of order p^4q^3 are associative if and only if $q \not\equiv 1 (\text{mod} p)$.

2 Definitions and Notations

The following definitions are quite standard. One can refer to [2,3,8] and [10] for further details.

1. A loop $\langle L, \cdot \rangle$, is a binary system that satisfies the following two conditions: (i) specification of any two of the elements x, y, z in the equation $x \cdot y = z$ uniquely determines the third element and (ii) the binary system contains an identity element (we denote it as 1).
2. A Moufang loop is a loop $\langle L, \cdot \rangle$ such that $(x \cdot y) \cdot (z \cdot x) = (x \cdot (y \cdot z)) \cdot x$ for any $x, y, z \in L$. (From now on, for the sake of brevity, we shall simply refer to the loop $\langle L, \cdot \rangle$ as the loop L. Also, we shall write $(x \cdot y) \cdot z$ simply as $xy \cdot z$, $(x \cdot (y \cdot z)) \cdot x$ as $(x \cdot yz)x$, etc.)
3. The associator subloop of L is denoted as $L_a = (L, L, L) = \langle (l_1, l_2, l_3) | l_i \in L \rangle$. In a Moufang Loop, L_a is the subloop generated by all the associators $(x, y, z) \in$

L such that $(x, y, z) = (x \cdot yz)^{-1}(xy \cdot z)$. It is obvious that L is associative if and only if $L_a = \{1\}$.

4. $I(L) = \langle R(x, y),\ L(x, y),\ T(x) | x, y \in L \rangle$ is called the inner mapping group of L, where

$$zR(x, y) = (zx \cdot y)(xy)^{-1},$$
$$zL(x, y) = (yx)^{-1}(y \cdot xz),$$
$$zT(x) = x^{-1} \cdot zx.$$

5. The commutator subloop of L, denoted L_c, is the subloop generated by all commutators $[x, y]$ in L, where $xy = yx \cdot [x, y]$.
6. The subloop generated by all $n \in L$ such that $(n, x, y) = (x, n, y) = (x, y, n) = 1$ for any $x, y \in L$ is called the nucleus of L. It is denoted as $N(L)$ or simply as N.
7. Suppose H is a subloop of L. Then $C_L(H) = \{g \in L | gh = hg \text{ for all } h \in H\}$.
8. Let M be a subloop of L and π a set of primes.
   (i) M is a normal subloop of L, denoted $M \triangleleft L$, if $M\theta = M$ for all $\theta \in I(L)$.
   (ii) A positive integer n is a π-number if every prime divisor of n lies in π.
   (iii) For each positive integer n, we let n_π be the largest π-number that divides n.
   (iv) M is a π-loop if the order of every element of M is a π-number.
   (v) M is a Hall π-subloop of L if $|M| = |L|_\pi$.
   (vi) M is a Sylow p-subloop of L if M is a Hall π-subloop of L and π contains only a single prime p.
9. Assume M is a normal subloop of L.
   (i) M is a proper normal subloop of L if $M \neq L$.
   (ii) L/M is a proper quotient loop of L if $M \neq \{1\}$.
10. Assume M is a normal subloop of L.
   (i) M is a minimal normal subloop of L if M is nontrivial and contains no proper nontrivial subloop which is normal in L. In other words, if there exists $H \triangleleft L$ with $\{1\} < H < M$, then $H = \{1\}$ or M.
   (ii) M is a maximal normal subloop of L if M is not a proper subloop of every other proper normal subloop of L. In other words, if there exists $H \triangleleft L$ such that $M < H$, then $M = H$ or $H = L$.
11. If m and n are integers, then (m, n) denotes the greatest common divisor of the two integers.

3 Basic Properties and Known Results

Let L be a Moufang loop.

Lemma 3.1 *L is diassociative, that is, $\langle x, y \rangle$ is a group for any x, y in L. Moreover, if $(x, y, z) = 1$ for some x, y, z in L, then $\langle x, y, z \rangle$ is a group.*
[3, Moufang's Theorem, p.117]

Lemma 3.2 *$N = N(L)$ is a normal subloop of L [3, Theorem 2.1, p.114]. Clearly N, is a group by its definition.*

Lemma 3.3 *Suppose $K \triangleleft L$.*

(a) If L/K is a group, then $L_a \subset K$.
(b) If L/K is commutative, then $L_c \subset K$. [15, Lemma 1, p.563]

Note that the properties above hold for all Moufang loops in general. However, the following properties hold only for finite Moufang loops L.

Lemma 3.4 *Suppose K is a subloop of L. Then $|K|$ divides $|L|$. [9, Lagrange's theorem, p.42]*

Lemma 3.5 *Suppose $|L|$ is odd, K is a subloop of L, and π is a set of primes.*

(a) Then L is solvable. [8, Theorem 16, p.413]
(b) If K is a minimal normal subloop of L, then K is an elementary abelian group and $(K, K, L) = \langle (k_1, k_2, l) | k_i \in K, l \in L \rangle = \{1\}$. [8, Theorem 7, p.402]
(c) If K is a normal subloop of L, $(K, K, L) = \{1\}$ and $(|K|, |L/K|) = 1$, then $K \subset N$. [8, Theorem 10, p.405]
(d) Then L contains a (Hall π-)subloop of order $|L|_\pi$. [8, Theorem 12, p.409]

Lemma 3.6 *L is a group if it has any of the following orders:*

(a) p, p^2, p^3 or pq where p and q are distinct primes. [6, Corollary 4 and Proposition 3, p.35]
(b) pqr or p^2q where p, q and r are distinct odd primes. [21, Theorem 3.1, p.124 and Theorem 3.3, p.126].
(c) p^4 where p is a prime and $p > 3$. [10, Theorem, p.33]
(d) pq^2 where p and q are distinct odd primes. [13, Theorem, p.269]
(e) $p_1 p_2 \cdots p_m q^3 r_1 r_2 \cdots r_n$ where $p_1, p_2, \cdots, p_m, q, r_1, r_2, \cdots, r_n$ are odd primes with $p_1 < p_2 < \cdots < p_m < q < r_1 < r_2 < \cdots < r_n$ and $q \not\equiv 1 (mod\ p_i)$ for all $i \in \{1, 2, \cdots m\}$. [23, Theorem 4.1, p.374]
(f) $p^\alpha q_1 \cdots q_n$, where $\alpha \leq 3$ and $p, q_1, \cdots, q_n$, are distinct odd primes with $p < q_i$. [12, Lemma 1,2, p.349, Theorem, p.350]
(g) $p^\alpha q_1 \cdots q_n$, where $\alpha \leq 4$ and $p, q_1, \cdots, q_n$, are distinct primes with $3 < p < q_i$. [15, Theorem, p.567]
(h) $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where $1 \leq \alpha_i \leq 2$ and $p_1, p_2, \cdots, p_n$ are distinct odd primes. [14, Theorem, p.882]
(i) $p^\alpha q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$, where p and q_i are primes with $p < q_1 < \ldots < q_n$ and $\beta_i \leq 2$ with $\alpha \leq 3$ when $p > 2$, or $\alpha \leq 4$ when $p > 3$. [16, Theorem 1, p.482 and Theorem 2, p.483]
(j) $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q^3$, where $p_1, p_2, \cdots, p_n$ and q are distinct odd primes with $q \not\equiv 1 (mod\ p_i)$ and $1 \leq \alpha_i \leq 2$. [24, Theorem 4.2, p.970]
(k) $p^3 q^3$, where p and q are odd primes with $p < q$, and $q \not\equiv 1 (mod\ p)$. [25, Theorem 4.6, p.1364]
(l) pq^4, where p and q are odd primes with $p < q$, and $q \not\equiv 1 (mod\ p)$. [5, Corollary 4.2, p.434]

Lemma 3.7 *Suppose $|L|$ is odd and every proper subloop of L is a group. If there exists a minimal normal Sylow subloop in L, then L is a group. [13, Lemma 2, p.268]*

Lemma 3.8 *If there exist H, K in L such that $H \triangleleft K \triangleleft L$ and $(|H|, |K/H|) = 1$, then $H \triangleleft L$. [14, Lemma 1, p.879]*

Lemma 3.9 *Let $|L| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q^{\beta}$, where $1 \leq \beta \leq 2$ and $p_1, p_2, \cdots, p_n$ are distinct odd primes such that $p_i < q$. Suppose:*

(i) every proper subloop of L is a group, and
(ii) there exists a Sylow q-subloop normal in L.

Then L is a group. [14, Lemma 3, p.879]

Lemma 3.10 *Let L be of odd order, K, a minimal normal subloop of L such that $K \subset L$, and Q, a Hall subloop of L. Suppose all proper subloops and proper quotient loops of L are groups, $(|K|, |Q|) = 1$ and $Q \triangleleft KQ$. Then L is a group. [15, Lemma 3, p.564]*

Lemma 3.11 *Let L be of odd order such that every proper subloop and proper quotient loop of L is a group. Suppose Q is a Hall subloop of L such that $(|L_a|, |Q|) = 1$ and $Q \triangleleft L_a Q$. Then L is a group. [15, Lemma 3, p.564]*

Lemma 3.12 *Let L be nonassociative and of odd order such that all proper quotient loops of L are groups. Then:*

(a) L_a is a minimal normal subloop of L [23, Lemma 1(a), p.478]; and is an elementary abelian group. [8, Theorem 7, p.402]
(b) if M is a maximal normal subloop of L, then L_a and L_c lie in M. Moreover, $L = M\langle x \rangle$ for any $x \in L \backslash M$. [23, Lemma 1(b), p.478]

Lemma 3.13 *Suppose K is a subloop of $C_L(L_a)$ and $(|K|, |L_a|) = 1$. Then $K \subset N$. [16, Lemma 5, p.480]*

Lemma 3.14 *Suppose*

(a) $|L| = p^{\alpha}m$ where p is a prime, $(p, m) = (p-1, p^{\alpha}m) = 1$ and L has an element of order p^{α}. Then there exists a (Sylow p-)subloop P of order p^{α} and a normal subloop M of order m in L such that $L = PM$.
(b) $|L| = p^2m$ where p is the smallest prime dividing $|L|$ and $(p, m) = 1$. Then there exists a subloop P of order p^2 and a normal subloop M of order m in L such that $L = PM$.

[17, Theorem 1, p.39]

Lemma 3.15 *Let L be of odd order and K a normal subloop of L. Suppose $K \subset N$. Then there exists a homomorphism from L to $Aut(K)$ with $C_L(K)$ as the kernel. Thus, $C_L(K) \triangleleft L$ and $|L/C_L(K)|$ divides $|Aut(K)|$. [11, Theorem 3(a), p.33]*

Lemma 3.16 *Let L be of odd order and K a normal Hall subloop of L. Suppose $K = \langle x \rangle L_a$ for some $x \in K \backslash L_a$ and $L_a \subset N$. Then $K \subset N$. [23, Lemma 3, p.17]*

Lemma 3.17 *Let L be nonassociative and of odd order, and let M be a maximal normal subloop of L. Suppose all proper subloops and proper quotient loops of L are groups. Then*

(a) L_a *is a Sylow subloop of* $N \implies L_a = N$. *[17, Lemma 6, p.480]*
(b) L_a *is cyclic* $\implies L_a \subset N$. *[16, Lemma 1, p.480]*
(c) $(k, w, l) = 1$ *for all* $k \in L_a, w \in M, l \in L \implies L_a \subset N$. *[16, Lemma 3, p.479]*
(d) $(k, w, l) \neq 1$ *for some* $k \in L_a, w \in M, l \in L \implies L_a$ *contains a proper nontrivial subloop which is normal in* M. *[23, Lemma 3, p.19]*

Lemma 3.18 *Suppose* $|L|$ *is odd and every proper subloop of* L *is a group. If* N *contains a Hall subloop of* L, *then* L *is a group. [15, Lemma 2, p.564]*

Lemma 3.19 *Let* L *be of order* $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q$, *where* $p_1, p_2, \cdots, p_n$ *and* q *are odd primes with* $p_1 < p_2 < \cdots < p_n < q$ *and* $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{Z}^+$, $q \not\equiv 1 (mod\ p_i)$ *for all* i. *Then there exists a normal subloop of order* $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ *in* L. *[25, Lemma 4.1, p.1362]*

Lemma 3.20 *Let* L *be nonassociative and of odd order, and let* M *be an associative maximal normal subloop of* L *and* P *be a subloop of* L . *Suppose* $L_a \subset N$ *and* $M = L_a P$. *Then for any* $x \in L \backslash M$, *there exist some* $r, s \in P$ *such that* $(x, r, s) \neq 1$. *[25, Corollary 4.3, p.1362]*

Lemma 3.21 *Let* L *be of odd order and* M *be an associative maximal normal subloop of* L. *Suppose* $L_a \subset N$. *Then* g *commutes with* (x, g, h) *for any* $x \in L \backslash M$ *and* $g, h \in M$. *[25, Lemma 4.4, p.1363]*

Lemma 3.22 *Suppose* p *and* q *are distinct odd primes. Then there exists a nonassociative Moufang loop of order* pq^3 *if and only if* $q \equiv 1 (mod\ p)$. *[22, Theorem 1, p.78 and Theorem 2, p.86]*

4 Main Results

Lemma 4.1 *Let* G *be a group and* $r, s, t \in G$ *with* $[r, t] = [s, t] = 1$. *Suppose* $r^{-1} s r = s^{\alpha} t^{\beta}$, *for some* $\alpha, \beta \in \mathbb{Z}^+$. *Then* $r^{-n} s r^n = s^{\alpha^n} t^{\beta(\alpha^0 + \alpha^1 + \cdots + \alpha^{n-1})}$ *for all* $n \in \mathbb{Z}^+$.

Proof (By induction.) Given $r, s, t \in G$ with $[r, t] = [s, t] = 1$ and $r^{-1} s r = s^{\alpha} t^{\beta}$ for some $\alpha, \beta \in \mathbb{Z}^+$. Let $P(n)$ be the statement $r^{-n} s r^n = s^{\alpha^n} t^{\beta(\alpha^0 + \alpha^1 + \cdots + \alpha^{n-1})}$ for $n \in \mathbb{Z}^+$.

When $n = 1$, $\alpha^{n-1} = \alpha^0$. So $\alpha^0 + \alpha^1 + \cdots + \alpha^{n-1} = \alpha^0 = 1$. Then $r^{-n} s r^n = r^{-1} s r = s^{\alpha^1} t^{\beta(1)} = s^{\alpha} t^{\beta}$. Hence $P(1)$ is true.

Assume that $P(k)$ is true for some fixed $k \in \mathbb{Z}^+$, i.e., $r^{-k} s r^k = s^{\alpha^k} t^{\beta(\alpha^0 + \alpha^1 + \cdots + \alpha^{k-1})}$.

Now

$$
\begin{aligned}
r^{-(k+1)} s r^{(k+1)} &= r^{-1} r^{-k} s r^k r \\
&= r^{-1} s^{\alpha^k} t^{\beta(\alpha^0 + \alpha^1 + \cdots + \alpha^{k-1})} r && \text{by } P(k) \\
&= r^{-1} s^{\alpha^k} r t^{\beta(\alpha^0 + \alpha^1 + \cdots + \alpha^{k-1})} && \text{since } [r, t] = 1 \\
&= (r^{-1} s r)^{\alpha^k} t^{\beta(\alpha^0 + \alpha^1 + \cdots + \alpha^{k-1})}
\end{aligned}
$$

$$
\begin{aligned}
&= (s^{\alpha}t^{\beta})^{\alpha^k} t^{\beta(\alpha^0+\alpha^1+\cdots+\alpha^{k-1})} && \text{by } P(1)\\
&= (s^{\alpha})^{\alpha^k} (t^{\beta})^{\alpha^k} t^{\beta(\alpha^0+\alpha^1+\cdots+\alpha^{k-1})} && \text{since } [s,t]=1\\
&= s^{\alpha^{(k+1)}} t^{\beta(\alpha^0+\alpha^1+\cdots+\alpha^k)}.
\end{aligned}
$$

Hence $P(k+1)$ is true. Then by the principle of induction, $P(n)$ is true for all $n \in \mathbb{Z}^+$.

This completes the proof of this lemma. □

(Note: This proof is obtained from the proof of lemma (4.5), p.1363 in [25], which proves it for Moufang loops with an associative subloop $\langle x, y, z\rangle$.)

Theorem 4.2 *Let L be a Moufang loop of order p^4q^3 where p and q are primes with $3 < p < q$, $q \not\equiv 1 (mod\ p)$. Then L is a group.*

Proof (By contradiction.)

$$\text{Assume there exists } L \text{ a nonassociative Moufang loop satisfying the conditions above.} \tag{4.1}$$

By lemma (3.5)(a), L is solvable. Also by Lagrange's theorem, every proper subloop and proper quotient loop of L is of order $p^{\alpha}q^{\beta}$ where $\alpha \leq 4$ and $\beta \leq 2$ or $p^{\alpha}q^3$, where $\alpha \leq 3$. All these proper subloops and proper quotient loops of L are associative by lemma (3.6)(h–k).

By lemma (3.12), L_a is a minimal normal subloop of L. Then by lemma (3.5)(b),

$$L_a \text{ is an elementary abelian group.} \tag{4.2}$$

So, $|L_a| = p,\ p^2,\ p^3,\ p^4,\ q,\ q^2$ or q^3.

If $|L_a| = p^4$ or q^3 then L_a would be a minimal normal Sylow subloop of L and so by lemma (3.7) L would be a group which contradicts assumption (4.1).

So, $|L_a| = p,\ p^2,\ p^3,\ q$ or q^2. We prove this theorem by considering the following four cases:

$|L_a| = q,\ |L_a| = q^2,\ |L_a| = p$ or p^2 and $|L_a| = p^3$. □

Case 1: $|L_a| = q$

By lemma (3.5)(d), there exists P a Hall subloop of order p^4 in L. Since $L_a \triangleleft L,\ L_aP < L$. So,

$|L_aP| = \frac{|L_a||P|}{|L_a \cap P|} = p^4q$. Since P is a Sylow p-subloop of L_aP, by lemma (3.19), $P \triangleleft L_aP$. Also, since $(|P|, |L_a|) = (p^4, q) = 1$, by lemma (3.10), L is a group. This contradicts assumption (4.1).

Case 2: $|L_a| = q^2$

By lemma (3.12) $L_a \triangleleft L$. Therefore, $|L/L_a| = p^4q$. Also by lemma (3.19), there exists a subloop $M/L_a \triangleleft L/L_a$ such that $|M/L_a| = p^4$. So $M \triangleleft L$.

$$\text{Hence } M \text{ is a maximal normal subloop of order } p^4q^2 \text{ in } L. \tag{4.3}$$

$$\text{Assume } (k, w, l) \neq 1 \text{ for some fixed } k, w, l \in L, \text{ with } k \in L_a \text{ and } w \in M. \tag{4.4}$$

Then by lemma (3.17)(d), L_a contains S a proper nontrivial subloop normal in M. Thus, $|S| = q$, so $|M/S| = p^4q$. Then by lemma (3.19), there exists $T/S \triangleleft M/S$ such that $|T/S| = p^4$, so $T \triangleleft M$ and $|T| = p^4q$. Again by lemma (3.19), there exists $R \triangleleft T$ such that $|R| = p^4$, since R is normal Hall subloop in T, by lemma (3.8) $R \triangleleft M$. Again by lemma (3.8), $R \triangleleft L$. Since L/R is a group, by lemma (3.3)(a), $L_a \subset R$. Then by lemma (3.4), $|L_a|$ is a divisor of $|R|$ which is a contradiction since $|L_a| = q^2$ and $|R| = p^4$.

Therefore, assumption (4.4) is false.

$$\text{Hence } (k, w, l) = 1 \text{ for all } k \in L_a, \text{ all } w \in M \text{ and all } l \in L.$$

By lemma (3.17)(c) $L_a \subset N$. So by lemma (3.4), $|L_a|$ is a divisor of $|N|$, i.e., $q^2 \mid |N|$. Also by lemma (3.18), N cannot contain any Hall subloop of L. So q^3 cannot divide $|N|$. Thus, L_a is a Sylow subloop of N. So by lemma (3.17)(a), $L_a = N$. Therefore, $|N| = q^2$.

$$\text{Now by lemma (3.15), } C_L(N) \triangleleft L \text{ and } |L/C_L(N)| \text{ divides } |Aut(N)|.$$

Suppose $p||C_L(N)|$. By Sylow's theorem there exists P a subloop of order p in $C_L(N)$. So $(|L_a|, |P|) = 1$ and by lemma (3.13), $P \subset N$. This is a contradiction since $p \nmid |N|$. Therefore,

$$p \nmid |C_L(N)|. \tag{4.5}$$

Now L_a is an abelian group by (4.2). Then by its definition, $C_L(L_a) = C_L(N)$ contains L_a. So $|L_a| = q^2$ is a divisor of $|C_L(N)|$ by lemma (3.4). Then by (4.5), $|C_L(N)| = q^2$ or q^3.

$$\text{Assume } |C_L(N)| = q^3. \tag{4.6}$$

Then for any $x \in C_L(N) \backslash L_a$, $|\langle L_a, x\rangle| > |L_a|$. But since $\langle L_a, x\rangle < C_L(N)$, $C_L(N) = C_L(L_a) = \langle L_a, x\rangle = \langle x\rangle L_a$. Now by lemma (3.15), $C_L(N)$ is a normal Hall subloop of L, so by lemma (3.16), we have that $C_L(N) \subset N$, which is impossible since $|C_L(N)| = q^3$ and $|N| = q^2$. So our assumption (4.6) is false. Therefore, $|C_L(N)| = q^2$. Then,

$$C_L(N) = N. \tag{4.7}$$

By (4.3) and lemma (3.5)(d), there exists a Sylow p-subloop

$$P \text{ of order } p^4 \text{ in } M. \tag{4.8}$$

Now $|L/M| = q$. So L/M is a group. Hence by lemma (3.3),

$$L_a \subset M \tag{4.9}$$

Since $L_a \lhd L$, by (4.8) and (4.9), $L_aP < M$ where $|L_aP| = \frac{|La||P|}{|L_a \cap P|} = q^2p^4 = |M|$. Hence $M = L_aP$. By lemma (3.20), we get that:

$$\text{for any } x \in L\backslash M \text{ there exists some } r, s \in P, \text{ such that } (x, r, s) \neq 1. \tag{4.10}$$

Now $|L_a| = q^2$, i.e., $L_a = N$ and by (4.2),

$$L_a = C_q \times C_q. \tag{4.11}$$

Write $t = (x, r, s)$. By, (4.11)

$$L_a = \langle t \rangle \times \langle u \rangle \tag{4.12}$$

for some $u \in L_a\backslash\langle t \rangle$. So by lemma (3.21)

$$[r, t] = 1, \tag{4.13}$$

since $P \subset M$ by (4.8).

The fact that $L_a \lhd L$ and $u \in L_a$ means $r^{-1}ur \in L_a$. So by (4.12) we can express

$$r^{-1}ur = u^{\lambda}t^{\eta} \tag{4.14}$$

for some $\lambda, \eta \in \mathbb{Z}^+$. Now $(u, t, r) = 1$ since $t \in L_a = N$. Thus, the elements u, t and r associate. So by lemma (4.1), we get that $u = r^{-|r|}ur^{|r|} = u^{\lambda^{|r|}}t^{\eta(\lambda^0+\lambda^1+\cdots+\lambda^{|r|-1})}$ since $|r| \in \mathbb{Z}^+$ as $r \neq 1$ by (4.10). Then $u^{1-\lambda^{|r|}} = t^{\eta(\lambda^0+\lambda^1+\cdots+\lambda^{|r|-1})} = 1$. Since $\langle t \rangle \cap \langle u \rangle = \{1\}$, $u^{1-\lambda^{|r|}} = 1$. So $q|(1 - \lambda^{|r|}) \implies \lambda^{|r|} \equiv 1 (\text{mod } q)$.

Now since $r \in P$, $|P| = p^4$ and $q \not\equiv 1 (\text{mod } p)$, $(|r|, q - 1) = 1$. It follows that the congruence $\lambda^{|r|} \equiv 1 (\text{mod } q)$ has only one solution for λ, i.e., $\lambda = 1$.

Now $\lambda^0 + \lambda^1 + \cdots + \lambda^{|r|-1} = \underbrace{(1 + 1 + \cdots + 1)}_{|r| \text{ times}} = |r|$. So $t^{\eta(\lambda^0+\lambda^1+\cdots+\lambda^{|r|-1})} = t^{\eta|r|} = 1$. Thus, $|t| = q$ divides $\eta|r|$. Since q is not a factor of $|r|$, $q|\eta$. This means $t^{\eta} = 1$. Hence $r^{-1}ur = u$ by (4.14), i.e., $[r, u] = 1$. So, by (4.12) and (4.13), r commutes with both generators of L_a. Therefore, $r \in C_L(L_a) = C_L(N) = N$ by (4.7). Then $(x, r, s) = 1$ by the definition of N. This is a contradiction since $(x, r, s) \neq 1$ by (4.10).

Therefore, $|L_a| \neq q^2$.

Case 3: $|L_a| = p^\mu, 1 \leq \mu \leq 2$.

By lemma (3.5)(d), there exists Q a Hall subloop of order q^3 in L. Since $L_a \triangleleft L$, $L_a Q < L$ where

$|L_a Q| = \frac{|L_a||Q|}{|L_a \cap Q|} = p^\mu q^3$. Since Q is a Sylow q-subloop of $L_a Q$, by lemma (3.14)(b), $Q \triangleleft L_a Q$. Since $(|Q|, |L_a|) = (q^3, p^\mu) = 1$, by lemma (3.10), L is a group. This again contradicts assumption (4.1).

Case 4: $|L_a| = p^3$

By lemma (3.12), $L_a \triangleleft L$. Since $|L/L_a| = pq^3$, by lemma (3.14), there exists a subloop $M/L_a \triangleleft L/L_a$ such that $|M/L_a| = q^3$. So $M \triangleleft L$ with $|M| = p^3 q^3$.

Hence M is a maximal normal subloop of L.

$$\text{Assume } (k, w, l) \neq 1 \text{ for some } k \in L_a, w \in M \text{ and } l \in L \tag{4.15}$$

By lemma (3.17)(d), L_a contains S a proper nontrivial subloop normal in M. Thus, $|S| = p^\gamma$, $1 \leq \gamma \leq 2$. So $|M/S| = p^{3-\gamma} q^3$, $1 \leq 3 - \gamma \leq 2$ and by lemma (3.14), there exists $T/S \triangleleft M/S$ such that $|T/S| = q^3$. So $|T| = p^\gamma q^3$ with $T \triangleleft M$. Again by lemma (3.14), there exists $R \triangleleft T$ such that $|R| = q^3$, and since R is normal Hall subloop in T, by lemma (3.8) $T \triangleleft M$. Again, since R is normal Hall subloop in M by lemma (3.8), $R \triangleleft L$. Since L/R is a group, by lemma (3.3)(a) $L_a \subset T$. Then by lemma (3.4), $|L_a|$ is a divisor of $|R|$ which is a contradiction since $|L_a| = p^3$ and $|R| = q^3$.

Therefore, assumption (4.15) is false.

Hence $(k, w, l) = 1$ for all $k \in L_a$, $w \in M$ and $l \in L$.

By lemma (3.17)(c) $L_a \subset N$. So by lemma (3.4), $|L_a| = p^3$ is a divisor of $|N|$. Also by lemma (3.18), N cannot contain a Hall subloop of L. So p^4 cannot divide $|N|$. Thus, L_a is a Sylow subloop of N. So by lemma (3.17)(a), $L_a = N$. Therefore, $|N| = p^3$.

Now by lemma (3.15), the subloop $C_L(N) \triangleleft L$ and $|L/C_L(N)|$ divides $|Aut(N)|$.

Assume $q||C_L(N)|$. Then, by Sylow's theorem there exists Q a subloop of order q in $C_L(N)$. So $(|L_a|, |Q|) = 1$ and by lemma (3.13), $Q \subset N$.

This is a contradiction since $q \not| |N|$. Therefore,

$$q \not| |C_L(N)|. \tag{4.16}$$

Now L_a is abelian by (4.2). Then by its definition, $C_L(N) = C_L(L_a)$ contains L_a. So $|L_a| = p^3$ is a divisor of $|C_L(N)|$.

So by (4.16), $|C_L(N)| = p^3$ or p^4. Assume $|C_L(N)| = p^4$. Then there exists $x \in C_L(N) \backslash L_a$ such that $\langle L_a, x\rangle < C_L(N)$ with $|\langle L_a, x\rangle| > |L_a|$, i.e., L_a is a proper subloop of $C_L(N)$. But since $\langle L_a, x\rangle < C_L(N)$, $C_L(N) = \langle L_a, x\rangle = \langle x\rangle L_a$. Now by lemma (3.15), $C_L(N)$ is a normal Hall subloop of L. So by lemma (3.16) we have that $C_L(N) \subset N$, which is impossible since $|C_L(N)| = p^4$ and $|N| = p^3$. So

$|C_L(N)| \neq p^4$. Therefore, $|C_L(N)| = p^3$, i.e., $C_L(N) = C_L(L_a) = L_a = N$. So $|L/C_L(L_a)| = pq^3$. Then by lemma (3.15),

$$pq^3 \text{ divides } |Aut(L_a)|. \tag{4.17}$$

Since $|L_a| = p^3$ in this case (i.e., case 4), $L_a = C_p \times C_p \times C_p$ by (4.2). Then by [1], $Aut(L_a) \cong GL(3, p)$ by simply viewing L_a as a vector space of dimension 3 over C_p, where $|GL(3, p)| = (p^3 - 1)(p^3 - p)(p^3 - p^2)$.

Therefore,

$$\begin{aligned} |Aut(L_a)| &= (p^3 - 1)(p^3 - p)(p^3 - p^2) \\ &= p^3(p^3 - 1)(p^2 - 1)(p - 1) \\ &= p^3(p - 1)^3(p + 1)(p^2 + p + 1). \end{aligned}$$

Then by (4.17), $q^3 | p^2(p - 1)^3(p + 1)(p^2 + p + 1)$.

Now $p - 1 < p < q \implies q \not| p$ and $q \not| (p - 1)$. Also $q \not\equiv 1 (\text{mod } p)$ $\implies q \not| (p + 1)$. Since q is a prime, $q \not| p^2(p - 1)^3(p + 1)$.

Therefore, $q^3 | (p^2 + p + 1)$ and so $q^3 \leq p^2 + p + 1 < p^2 + 2p + 1 = (p + 1)^2$.

Thus,

$$q^3 < (p + 1)^2. \tag{4.18}$$

However, since both p and q are odd primes, with $p < q$, $p+2 \leq q \implies p+1 < q$. So $(p + 1)^2 < q^2$. Then we have by (4.18) that $q^3 < q^2$ which is a contradiction.

Therefore, $|L_a| \neq p^3$.

Since each case 1, 2, 3 and 4 ended with a contradiction, we conclude that assumption (4.1) is false. Hence L is a group.

5 Open Problem

In view of lemma (3.6) (l) and theorem (4.2), the next unsolved case is Moufang loops of order p^2q^4 where p and q are odd primes with $p < q$ and $q \not\equiv 1 (\text{mod} p)$. Recently we have obtained a partial result for this problem by adding a sufficient—but perhaps unnecessary—condition $q \not\equiv -1 (\text{mod} p)$ and proving that all such Moufang loops are associative. Due to the difficulty we face in proving associativity without this added condition, we are making a bold (but perhaps untrue) conjecture:

"There exist (a class of) nonassociative Moufang loops of order p^2q^4 where p and q are odd primes with $p < q$, $q \not\equiv 1 (\text{mod} p)$ but $q \equiv -1 (\text{mod} p)$."

If our conjecture is true, there would exist a nonassociative Moufang loop of order $3^2 5^4$—the smallest one satisfying the given conditions.

This class would contain only minimally nonassociative Moufang loops since every proper subloop and every proper quotient loop of this loop would be a group by lemma (3.6) (e) and (l).

References

1. Adney, J.E., Yen, T.: Automorphism of p-groups. Ill. J. Math. **9**, 137–143 (1965)
2. Bol, G.: Gewebe und gruppen. Math. Ann. **114**(1), 414–431 (1937)
3. Bruck, R.H.: A Survey of Binary Systems, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie Springer, Berlin, (1958)
4. Chee, W.L., Gagola III, S.M., Rajah, A.: Classification of minimal nonassociative Moufang loops of order pq^3. Int. J. Algebra **8**, 1895–1908 (2013)
5. Chee, W.L., Rajah, A.: Moufang loops of odd order pq^4. Bull. Malays. Math. Sci. Soc. **37**(2), 425–435 (2014)
6. Chein, O.: Moufang loops of small order. I. Trans. Amer. Math. Soc. **188**(2), 31–51 (1974)
7. Chein, O., Rajah, A.: Possible orders of nonassociative Moufang loops. Comment. Math. Univ. Carolin. **41**(2), 237–244 (2000)
8. Glauberman, G.: On loops of odd order. II. J. Algebra **8**, 393–414 (1968)
9. Grishkov, A.N., Zavarnitsine, A.V.: Lagrange's theorem for Moufang loops. Math. Proc. Cambridge. Philos. Soc. **139**(1), 41–57 (2005)
10. Leong, F.: Moufang loops of order p^4. Nanta Math. **7**(2), 33–34 (1974)
11. Leong, F.: The devil and angel of loops. Proc. Am. Math. Soc. **54**, 32–34 (1976)
12. Leong, F., Lim, V.K.: Moufang Loops of odd order $p^m q_1 \cdots q_n$. J. Algebra **168**(1), 348–352 (1994)
13. Leong, F., Rajah, A.: On Moufang loops of odd order pq^2. J. Algebra **176**(1), 265–270 (1995)
14. Leong, F., Rajah, A.: Moufang loops of odd order $p_1^2 p_2^2 \cdots p_m^2$. J. Algebra **181**(3), 876–883 (1996)
15. Leong, F., Rajah, A.: Moufang loops of odd order $p^4 q_1 \cdots q_n$. J. Algebra **184**(2), 561–569 (1996)
16. Leong, F., Rajah, A.: Moufang loops of odd order $p^\alpha q_1^2 \cdots q_n^2 r_1 \cdots r_m$. J. Algebra **190**(2), 474–486 (1997)
17. Leong, F., Rajah, A.: Split extension in Moufang loops. Publ. Math. Debr. **52**(1–2), 33–42 (1998)
18. Nagy, G.P., Valsecchi, M.: On nilpotent Moufang loops with central associators. J. Algebra **307**(2), 547–564 (2007)
19. Nagy, G.P., Vojtechovsky, P.: The Moufang loops of order 64 and 81. J. Symb. Comput. **42**, 871–883 (2007)
20. Pflugfelder, H.O.: Quasigroups and Loops: Introduction. Heldermann, Berlin (1990)
21. Purtill, M.: On Moufang Loops of odd order the product of three odd primes. J. Algebra **112**(1), 122–128 (1988)
22. Rajah, A.: Moufang loops of odd order pq^3. J. Algebra **235**, 66–93 (2001)
23. Rajah, A., Chee, W.L.: Moufang loops of odd order $p_1 p_2 \cdots p_n q^3$. Bull. Malays. Math. Sci. Soc. **34**(2), 369–377 (2011)
24. Rajah, A., Chee, W.L.: Moufang loops of odd order $p_1^2 p_2^2 \cdots p_n^2 q^3$. Int. J. Algebra **5**, 965–975 (2011)
25. Rajah, A., Chee, W.L.: Moufang loops of odd order $p^3 q^3$. Int. J. Algebra **8**, 1357–1367 (2011)
26. Wright, C.R.B.: Nilpotency conditions for finite loops. Ill. J. Math. **9**, 399–409 (1965)